■研究調査レビュー

中小企業の情報セキュリティ対策の現状

下園　幸一（鹿児島大学法文学部）

１　企業の情報化の現状

1970年代以降ＰＣ（パーソナル・コンピュータ）の普及とともに，我々の社会には多くの場面でコンピュータが取り入れられ，生活にとって必要不可欠なものとなっている。こうした環境のなか，企業のＯＡ化の動きは早く，国内企業の98％が既にコンピュータ機器の導入を果たしている。平成16年３月「鹿児島県内中小企業のコンピュータ機器及びインターネット利用状況調査」によると，企業が社内業務においてコンピュータを利用する目的は，「文書作成・表計算」（94.7％）が最も多く，次いで「財務会計」（75.3％），「社内外へのネットワーク・インターネット」（65.6％）となっており，いまやＰＣで事務処理や会計計算を行なうことは，企業にとって珍しいことではなくなった（[図１］参照)。

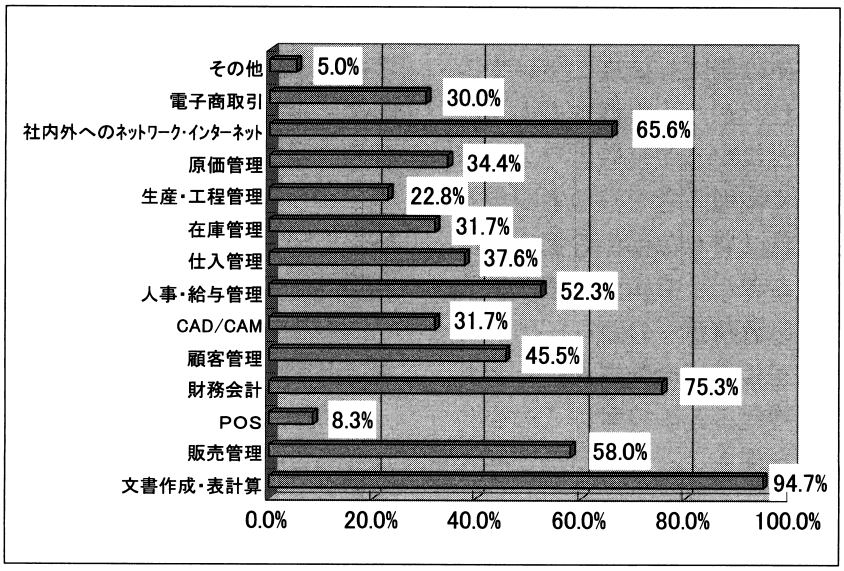

図１．鹿児島県内中小企業のコンピュータ機器の利用目的

また，情報通信ネットワークに関しては，近年普及の動きが急速化している。総務省の「平成15年通信利用動向調査の結果」によると，インターネットの普及率が，企業・事業所いずれも高い数値を示していることがわかる（[図２］参照)。ADSLや光ファイバをはじめとするブロードバンド回線が一般家庭にも定着化したことが，一般世帯の普及率上昇につながっている。

その一方で，企業は以前から比較的高い普及率を維持してきた。1990年代前半，日本でインターネットサービスが開始されると，それとともに多くの企業がそれまでの企業形態を変え始めた。SCMの構築や電子商取引を経営に取り入れる企業もその数を増やしている。さらに，専用回線や光ファイバによって，情報通信の高速化・安全性が高められたことも普及を手助けしていると言える。この

ような背景から，多くの人が，インターネットをはじめとする情報通信ネットワークを通じて，整理された情報を距離の制限を受けずにやり取りできるようになった。

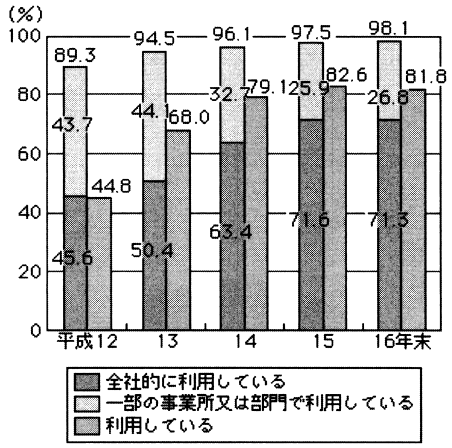

図２．企業・事業所別インターネットの普及率（左：企業，右：事業所）

「鹿児島県内中小企業のコンピュータ機器及びインターネット利用状況調査」では，インターネットの利用目的［図３］に関して，現在では９割以上の企業で「電子メールの利用」（91.4%）が可能である。その他に「データ・ファイルの転送」（51.7%）や「仕入業務の情報収集」（46.9%）など，他社との情報交換という場面において，ネットワークの導入は大きく貢献している。

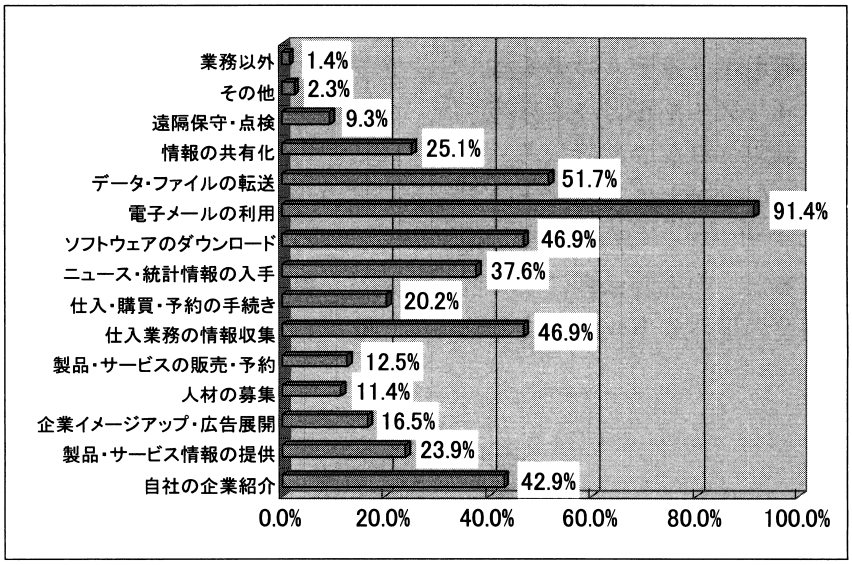

図３．鹿児島県内中小企業のインターネットの利用目的

2　情報セキュリティ被害の現状

インターネットの普及は，距離の制限なく多くの情報を得られる上，遠方との情報交換を可能にしたと先に述べた。しかし，逆の言い方をすると，インターネットの普及は，誰もが，どこからでも他者の情報にアクセスで

きてしまう危険を生んだ。

「平成17年版情報通信白書」によると，平成16年の１年間に情報通信ネットワーク（インターネットや企業通信網）の利用において，83.5％の企業が情報セキュリティに関する何らかの被害を受けたと報告された。被害内容は，「ウイルス感染・発見」が最も多く，被害全体の66.4％にのぼる。また，実際にウイルスに感染した企業は32.6％にのぼる。そして，「不正アクセス」（9.1％），「スパムメールの中継利用・踏み台」（6.3％）と続いている（[図４］参照)。

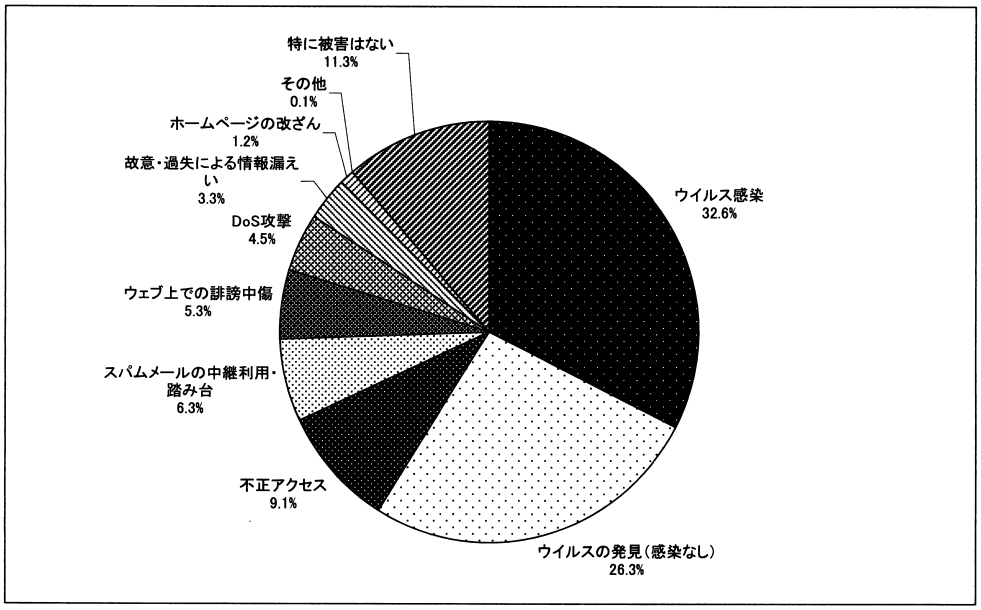

図４．平成16年における企業の情報通信ネットワークの被害状況

企業における情報セキュリティの脅威は，コンピュータ・ウイルスや不正アクセス等，外部からのものに制限されない。むしろ，内部関係者の故意あるいは過失による被害の方が，リスクが高いのである。「平成15年版情報通信白書」によると，内部関係者による情報セキュリティ関連の事件や事故が発生した企業は，14.7％と発生率は２割以下だ（[図５］参照)。その内容を［図６］に示す。この図によると「権限を越えた情報・サービスへのアクセス」が最も多く，「コンピュータ等ハードウェアの窃盗，破壊」がそれに続いており，悪質なものが目立つ。

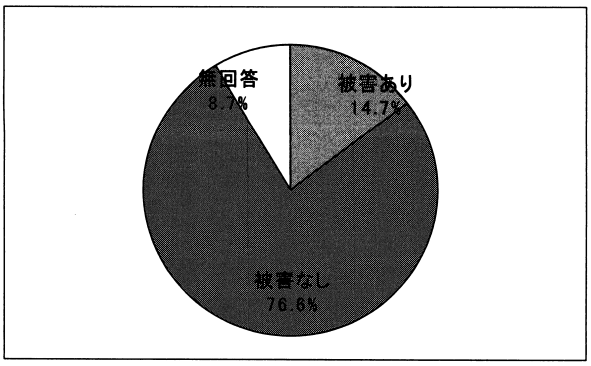

図５．平成14年における企業の内部要因による情報セキュリティ被害状況

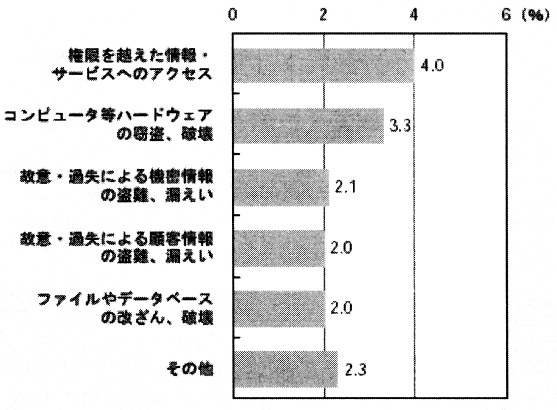

図６．平成14年における企業の内部要因による情報セキュリティ被害内容

３　続発する企業からの情報漏えい

コンピュータの処理能力の向上は，企業が顧客データをデータベース化し，様々な目的のために二次利用することを可能にした。また，コンピュータがネットワークとつながり，購買履歴などのデータがリアルタイムで蓄積されることで，企業はより詳細な個人情報を把握することができるようになった。

その一方で，ニュースなどによる報道で，企業による情報漏えいが多く取り上げられ，世間の注目が集まっている。「インターネット白書2004」によると，2002年１月から2004年３月には，「ジャパネットたかた」や「ローソン」といった大手企業の個人情報漏えいが目立ち，個人情報の取扱いに対する社会的不安の増加に拍車をかけた（[表１]参照)。また，個人情報の漏えいによって生じた被害者の合計人数は，2003年１年間だけでも155万4,592人。損害賠償総額は，損害賠償金や，ブランドイメージの低下等による売上げへの影響まで考慮すると，280億6,936万円にも及ぶ。

こうした「個人情報の利用の増加」と「情報漏えい急増への不安」を背景に，2003年５月30日に制定，交付された「個人情報保護法」が2005年４月より全面施行されている。これは，個人の権利と利益を保護するために，個人情報を取り扱っている事業者に対し，様々な義務と対応を定めた法律である。この法律は，以下の５つの原則から成り立つ。

・利用方法による制限：利用目的を本人に明示
・適正な取得：利用目的の明示と本人の了解を得て取得
・正確性の確保：常に正確な個人情報に保つ
・安全性の確保：流出や盗難，紛失を防止する
・透明性の確保：本人が閲覧可能，本人への開示が可能，本人の申出により訂正を加えられる，同意なき目的外利用は本人の申し出によって停止できる

これにより，国の定める一定数以上の従業員をもつ企業や，大量のカルテを有する医療機関など，個人情報をデータベース化する事業者は，個人情報を第三者に提供する際に，利用目的を本人に通知し了解を得なくてはならない。また，不正流用防止のための管理を行う義務も発生する。もし，これを守らなければ，情報主体（本人）の届出や訴えにより，最高で事業者に刑罰が科される。したがって，個人情報の売買やそれに準ずる行為を行う名簿業者などは，その存在を完全に否定されるだろう事が予測されている。

しかし，情報主体（個人）が苦情処理機関

又は当該事業者に訴えでない限り，個人情報保護法が実効性をもつことは皆無であり，企業をはじめ事業者がこの法律に沿って個人情報を取り扱うかは疑問が残る。

表１．おもな個人情報漏えい事件（2002年－2004年３月）

報道年月日	個人情報漏えい事例
2004年 ３月	東武鉄道のメール・マガジン「102@Club」会員の情報が，最大で約13万2,000件漏えいした。
３月	ADSL事業者のアッカ・ネットワークスは，110万人分の顧客情報が漏えいした可能性があると認めた。
２月	通販大手のジャパネットたかたの顧客情報が，最大で66万人分漏えいした。
１月	Yahoo! BB 加入者451万人分の個人情報が記録されたDVD－ROMを入手した男が，ソフトバンクグループ企業関係者から数十億円を脅し取ろうとし，恐喝未遂で逮捕された。
2003年 10月	ファミリーマートの「ファミマ・クラブ」会員メール・マガジン購読者約18万人分の情報が流出した。
８月	信販大手のアプラスから，クレジットカードの分割払を利用している顧客７万9,000人の名前や年収区分などの個人情報が，ダイレクトメール会社2社に流出した。
８月	鳥取県は，同県のホームページ「とりネット」上で，県行事の応援者89人と，韓国人の訪日団員39人の住所，電話番号などの個人情報を約９～５ヵ月にわたって公開していた。さらに，発覚後，削除指示ミスにより，引き続き公開して“二次流出”した。
６月	ローソン及び関連会社が発行しているローソンパス会員カードの顧客情報（氏名，住所，性別，生年月日，自宅電話番号，携帯電話番号）約56万件が社外に流出した。
３月	東京農工大の入学予定者ら950人分の氏名，生年月日，性別，学科名，受験番号などの個人データが入ったフロッピーディスクと書類を，同大から入学手続のデータ入力業務を委託された情報処理会社の社員が通勤途中の電車内に置き忘れて紛失した。
３月	長野県赤十字血液センターで，県内の献血者70人以上の氏名や血液型などの個人情報を，元派遣社員が別会社の顧客名簿に使用した。
２月	楽天の子会社の検索サイトinfo seekのメール転送サービスで，一部のメールが利用者本人以外の第三者に転送される問題が発生した。
２月	河合塾は，大学入試センター試験の模擬試験を受験した高校生の成績や学校名などの個人情報が同塾の職員から別の予備校に流出したことを公開した。
１月	駿台予備校は，同校の提供する合否シミュレーションサービスの一部の受験生の成績情報が第三者から閲覧可能な状態にあったことを公表した。
2002年 12月	福島県岩代町で，全町民約9,600人分の個人情報が漏えいした。住民票コードを含む15項目の個人情報が記載されていた。
11月	東京経済大学の受験生3,107人分の個人情報が1年以上にわたってインターネットで検索可能な状態になっていた。
10月	筑波大学の学務システムに登録されていた全学生の顔写真が閲覧可能状態になっていた。
７月	インターネットカフェ会員１万7,000人分のリストが閲覧可能になっていた。
７月	アビバのWebサイトから約1,200人分の個人情報が流出した。
６月	消費者金融大手のライフが，クレジットカード利用明細書2600人分を誤送付した。
５月	TBCのWebサイトから約３万人分の個人情報が漏えいした。
１月	静岡朝日テレビが，1,900人の視聴者にメールを配信する際に，他の視聴者のメールアドレスも一緒に送信した。

（出展　インターネット白書2004）

4　企業における情報セキュリティ対策の取り組み

日々，増加する情報セキュリティ被害に対し，企業のとる情報セキュリティ対策について見ていく。2002年の総務省「情報セキュリティ対策の状況調査結果（中小企業向け）」を参考に，大企業と中小企業それぞれの情報セキュリティ対策の導入率の比較を行なった。すると，いずれをとっても中小企業に比べ，大企業の方がセキュリティ対策に積極的な姿勢をとっていることが分かる。

なかでも，ファイアウォールについては，大企業の約87％が実施済みであるのに対し，中小企業の導入率は約46％にとどまっている。また，企業のセキュリティに対する基本的な考え方やファイアウォールの適正な運用等の具体的な対策を明文化したセキュリティポリシーについても，大企業の策定率は約43％に達するが，中小企業の策定率は約18％とその差は大きい（[表2］参照)。

表2．大企業，中小企業別情報セキュリティ対策の導入率

	大企業（％）	中小企業（％）
ファイアウォールの設置	86.9	46.4
セキュリティポリシーの策定	42.8	18.5
ウイルス対策ソフト	95.2	77.2
IDSの導入	17.6	9.6
VPN[1]（VPNによるアクセス制限）	19.8	7.5

（大企業≧社員300人≧中小企業）

一方，クライアント用のウイルス対策ソフトは，最近ではＰＣにバンドルされていることもあり，大企業の導入率は約95％，中小企業の導入率も約77％と比較的高水準である。しかし，ウイルス対策ソフトを正しく利用しているとは限らない。

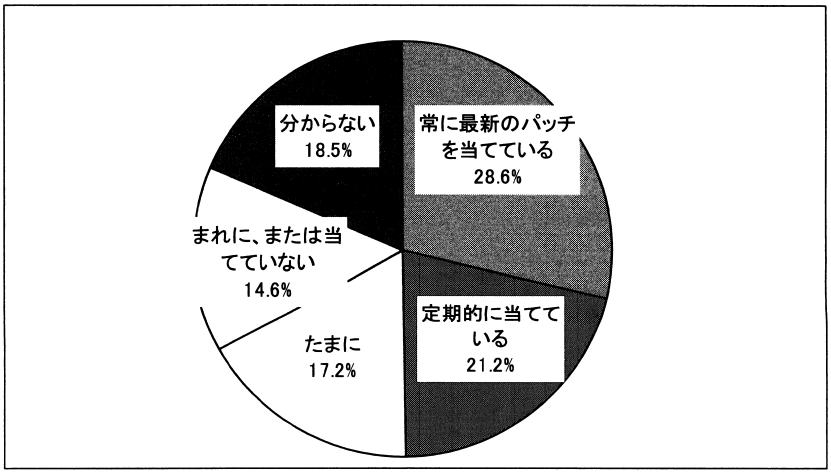

図7．企業におけるウイルス対策ソフトのセキュリティパッチ適用頻度

［図7］より，民間企業のウイルス対策ソフトのセキュリティパッチ適用頻度を見ると，「常に最新のパッチを当てている」若しくは「定期的に当てている」のは全体の50％にも満たない。セキュリティパッチの適用がエンドユーザ個人で行われることが多く，作業が怠慢になってしまうからである。しかし，その一方で，セキュリティデータを更新することにより，既存の情報システムが正常に機能しなくなることを危惧して，敢えてパッチを当てない企業もある。本来，こうした動作チェックは，情報システムのデータが更新される度に行われるものであるが，これらを実施する時間的・金銭的余裕のない企業がパッチを当てないまま業務を続けてしまう現状がある。

このような現状では，ウイルス対策ソフトをクライアント用ＰＣに入れていても，十分な対策が講じられているとは言えない。ウイルス対策ソフトの利用に関しては，自己対策の促進を含め，危機意識の強化という部分において，課題が残されているように感じる。

中小企業の情報セキュリティ導入率が，大企業と比べて低いことは先の図で見ることができたが，今度は情報セキュリティ対策を行っていない企業の立場に立って，なぜセキュリティ対策が積極的に行われないのか，その理由について考えていく。

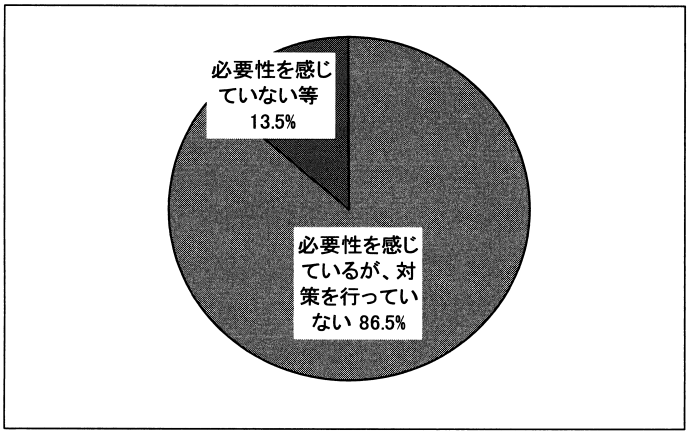

図８．情報セキュリティ未実施者の意識

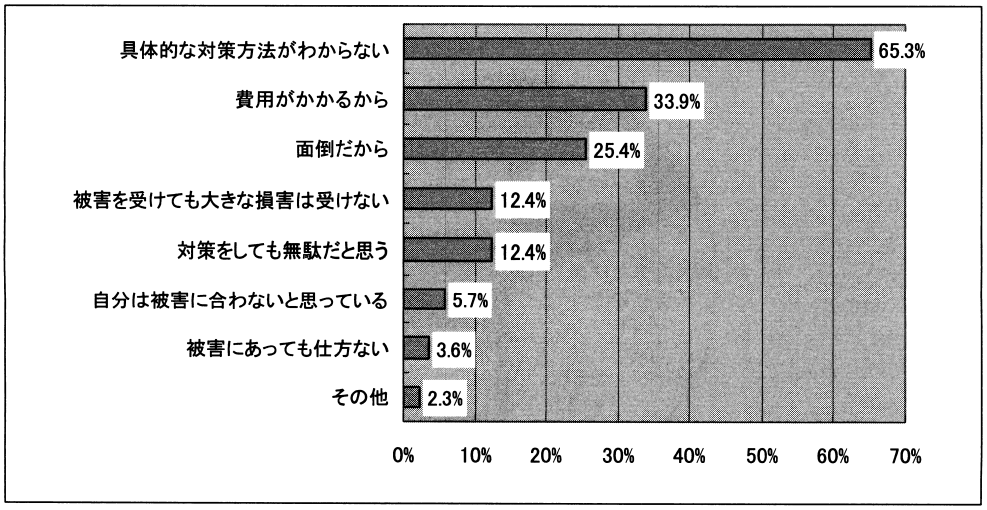

図９．情報セキュリティ対策に取り組まない理由（複数回答）

総務省「平成15年版情報通信白書」によると，情報セキュリティ未実施者の意識としては，その多くがセキュリティの必要性を感じており，「具体的な対策方法がわからない」（65.3%），「費用がかかる」（33.9%）といった理由から，セキュリティ対策に取り組めないでいる傾向が強い。しかし，「面倒だから」（25.4%），「被害を受けても大きな損害は受けないだろう」（12.4%）という企業経営者による危機意識の低さから情報セキュリティ対策を実施しないという意見も目立った（[図8］[図9］参照)。

特に，「具体的なノウハウが分からない」といった問題に対し，ISOやBSIは，企業・団体向けの情報システムセキュリティ管理のガイドラインを発表し，組織のセキュリティレベルの向上を推進している。その代表的なものに，ISO／IEC15408とBS7799がある。

ISO／IEC15408は，セキュリティ製品（ハード・ソフトウェア）及びシステムの開発や製造，運用などに関する国際標準で，情報セキュリティ評価基準として1999年6月に採択された。この規格では，セキュリティの確保に必要な機能や信頼性が分類されており，国際的に通用する基準に基づいてセキュリティレベルを評価することが可能となっている。

一方，BS7799は，BSIによって定められた規格である。組織の情報セキュリティマネジメントや手順の適正を評価及び認証する仕組みが作られており，情報セキュリティマネジメントの国際基準として高い注目を浴びている。なお，BS7799は情報セキュリティの運用管理に重点が置かれ，セキュリティマネジメントの規格としての意味合いが強いことから，セキュリティポリシー策定のための規格として，広く認識されている。

これら2つの規格が標準化されたことからも，情報セキュリティ対策の重要度は確実に高まっており，企業の積極的な取り組みが求められる。

5　おわりに

コンピュータ・ウイルスやワーム感染，不正アクセスといった情報セキュリティ被害は，社会の情報化促進と比例して年々その数を増やしてきた。いまや，情報システムを有する企業にとって，システムの利便性のみを追求するだけでは，業務を安全かつ効率的に進めることが困難な時代になったといえる。

社会で情報セキュリティの危機意識が高まる一方，中小企業の情報セキュリティ対策はまだ万全とは言えない。確かに，今までは情報セキュリティ対策製品の導入について，費用対効果が見えにくいことや，経営者がノウハウを理解できていないままシステムを取り入れてきた背景があった。今後は，より拡大していくだろう情報セキュリティ被害をより身近にあるものとして捉え，その対策に積極的に取り組んでいく姿勢が強く求められる。それは単に情報セキュリティ対策製品の導入のみならず，セキュリティポリシーや社内規定といった社員一人一人の心構えまでも含む。不正アクセス被害の大半は，設定ミスや操作ミスにその原因があるという。悪意をもった人間が簡単に情報システムにアクセスできてしまう隙を見せないよう，管理体制を充実させた上で，有効に情報セキュリティ対策製品を利用していくことが大切である。

自社のシステムさえ保持しきれない企業を消費者や顧客は信頼しない。この意識をもって，セキュリティ対策に取り組む企業が増えてくれることを望む。